

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for: Calendar Year 2018

Name of companies covered by this certification:

Atlantic Broadband (CT), LLC	Form 499 Filer ID: 831128
Atlantic Broadband (Delmar), LLC	Form 499 Filer ID: 831131
Atlantic Broadband (Miami), LLC	Form 499 Filer ID: 831132
Atlantic Broadband Enterprise, LLC	Form 499 Filer ID: 830062
Atlantic Broadband (Penn), LLC	Form 499 Filer ID: 831130
Atlantic Broadband (NH-ME), LLC	Form 499 Filer ID: 826014
Atlantic Broadband (SC), LLC	Form 499 Filer ID: 831129
Atlantic Broadband Finance, LLC	Form 499 Filer ID: 826014

Name of Signatory: Leslie Brown

Title of Signatory: Senior Vice President / General Counsel / Secretary

I, Leslie Brown, as an officer of the above stated companies, certify and state that:

I am the Senior Vice President / General Counsel / Secretary of Atlantic Broadband (CT), LLC; Atlantic Broadband (Delmar), LLC; Atlantic Broadband (Miami), LLC; Atlantic Broadband Enterprise, LLC; Atlantic Broadband (Penn), LLC; Atlantic Broadband (NH-ME), LLC; Atlantic Broadband (SC), LLC; and Atlantic Broadband Finance, LLC (collectively, the "Atlantic Broadband Companies") and, acting as an officer and agent of each of the Atlantic Broadband Companies, I have personal knowledge that the Atlantic Broadband Companies have established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Atlantic Broadband Companies' procedures ensure that the Atlantic Broadband Companies are in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in Section 64.2001 *et seq.* of the Commission's rules.

The Atlantic Broadband Companies have not taken any actions (i.e., proceedings instituted or petitions filed by the Atlantic Broadband Companies at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The Atlantic Broadband Companies have not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The Atlantic Broadband Companies represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The Atlantic Broadband Companies also acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject them to enforcement action.



Leslie Brown

Sr. Vice President/General Counsel/Secretary

Atlantic Broadband (CT), LLC; Atlantic Broadband (Delmar), LLC; Atlantic Broadband (Miami), LLC; Atlantic Broadband Enterprise, LLC; Atlantic Broadband (Penn), LLC; Atlantic Broadband (NH-ME), LLC; Atlantic Broadband (SC), LLC; Atlantic Broadband Finance, LLC

Executed February 27, 2019

ACCOMPANYING STATEMENT
ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

The following summary describes the policies of Atlantic Broadband Finance, LLC and its subsidiaries (collectively, "ABB") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

1. Use and Disclosure of CPNI

ABB has adopted specific CPNI policies to ensure that it may only use, disclose, or permit access to individually identifiable CPNI in connection with its provision of the telecommunications service from which the information is derived or services necessary to, or used in, the provision of the telecommunications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; to protect ABB's rights or property; as expressly authorized by the customer; or as otherwise permitted by law and regulation.

ABB does not use, disclose, or permit access to CPNI to market service offerings to a customer that are not within a category of service to which the customer already subscribes. In the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process. If such use is approved, ABB shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules, including obtaining required prior approvals from customer prior to the use or disclosure of CPNI for which such approval is required by FCC rules.

ABB does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When ABB receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

2. Company Safeguards to Protect CPNI

ABB and its employees will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. ABB has established procedures and trains personnel so customers are properly authenticated before accessing CPNI based on customer-initiated telephone contact, online account access or an in-store visit, in accordance with Section 64.2010

(b)-(d) of the Commission's rules. For inbound caller requests for call details, for instance, ABB requires customers to verify their account using a PIN (defined below) prior to disclosing any such call details. In person, ABB may disclose a customer's CPNI to an authorized person only upon verifying that person's identity through a valid, non-expired government-issued photo ID matching the customer's account information.

ABB will authenticate a customer without the use of readily available biographical information or account information prior to the customer establishing a password or in the case of a lost or forgotten password. Authentication is accomplished through the use of a Personal Identification Number ("PIN"). The PIN is randomly generated and supplied to new customers at service initiation. For existing customers, PINs were mailed to the address of record. Additionally customers will establish a backup authentication method that does not prompt the customer for readily available biographical information or account information. Customers that cannot provide the correct PIN or the correct response to their back-up authentication method must establish a new PIN, which can be achieved by either (a) a call by ABB to the phone number of record to provide the existing PIN or to set a new PIN, or (b) having ABB send the PIN to the customer's address of record.

ABB will notify the customer when there are account changes, such as change of password, backup authentication information, or address of record. Whenever a Customer's password or address of record is created or changed, ABB sends a notice to customer's pre-existing address of record and/or by voicemail to the telephone number of record notifying them of the change. The notice provided under this paragraph will not reveal the changed information and will direct the customer to notify ABB if they did not authorize the change.

ABB has trained its personnel with access to CPNI as to when they are and are not authorized to use CPNI, and has adopted and communicated an express disciplinary process. Any improper use shall be treated as a serious offense, and may result in suspension or termination of employment in appropriate cases. Any company personnel making improper use of CPNI will undergo additional training to ensure future compliance. ABB will provide additional training on an as-needed basis.

An ABB officer, as an agent of the company, signs and files with the FCC a compliance certificate on or before March 1 of each year stating that the officer has personal knowledge that ABB has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

ABB will take additional steps to protect the privacy of its customers' CPNI and to discover and protect against activity that is indicative of pretexting.

3. Business Customer Exemption

ABB may use different authentication methods for a business customer if such methods are contractually binding, the negotiated service contract specifically discloses ABB's policy to protect CPNI, and the customer has a dedicated ABB account representative.

4. Notification of any CPNI Security Breach

A “breach” of CPNI has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, ABB shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. ABB will not notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI, and will defer such notification at the request of either agency. If ABB receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed in the breach.

5. Recordkeeping

ABB will maintain separate files in which it will retain any court orders respecting CPNI.

ABB will maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

ABB maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If ABB later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission’s recordkeeping requirements.

ABB maintains a record of all customer complaints related to their handling of CPNI, and records of ABB’s handling of such complaints, for at least two years. All complaints are reviewed and ABB will consider any necessary changes to its policies or practices to address the concerns raised by such complaints.